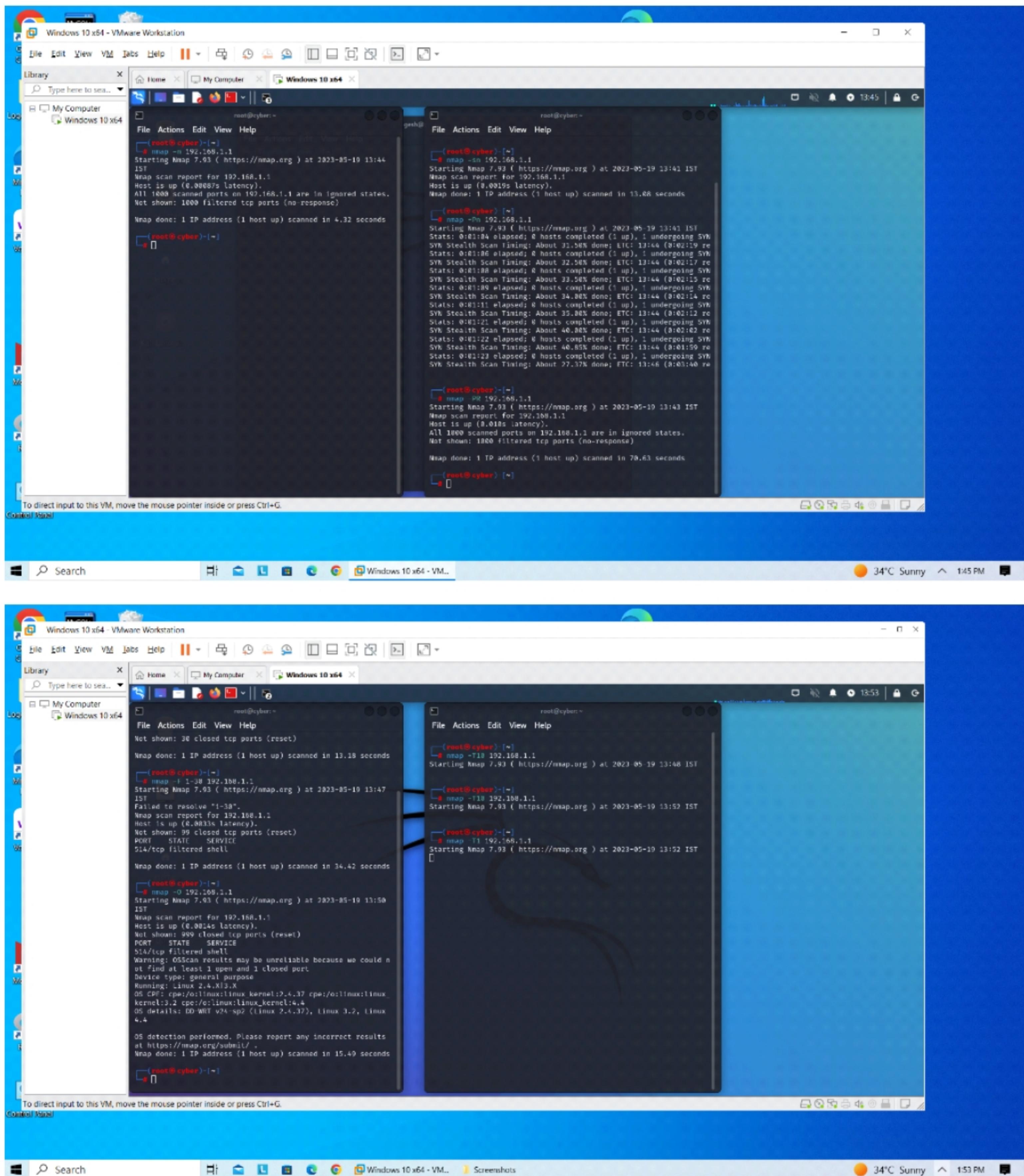


## 1. network map sacnning



The image shows a Windows 10 desktop environment within a VMware Workstation window. There are three terminal windows open, all running as root on a host named 'cyber'. Each terminal window displays the output of an nmap scan against the IP address 192.168.1.1.

```
# nmap -n 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-19 13:44
IST
Nmap scan report for 192.168.1.1
Host is up (0.0008s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1800 filtered tcp ports (no response)

Nmap done: 1 IP address (1 host up) scanned in 4.32 seconds

# nmap -sn 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-19 13:41 IST
Nmap scan report for 192.168.1.1
Host is up (0.0019s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1800 filtered tcp ports (no response)

Nmap done: 1 IP address (1 host up) scanned in 13.08 seconds

# nmap -O 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-19 13:43 IST
Nmap scan report for 192.168.1.1
Host is up (0.018s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1800 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 70.63 seconds
```

Below the terminals, the Windows taskbar shows the date and time as 145 PM, and the system tray indicates a temperature of 34°C and sunny weather.

```
# nmap -O 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-19 13:47 IST
Failed to resolve "1-38".
Nmap scan report for 192.168.1.1
Host is up (0.001ms latency).
Not shown: 99 closed tcp ports (reset)
PORT      STATE      SERVICE
514/tcp   filtered  shell

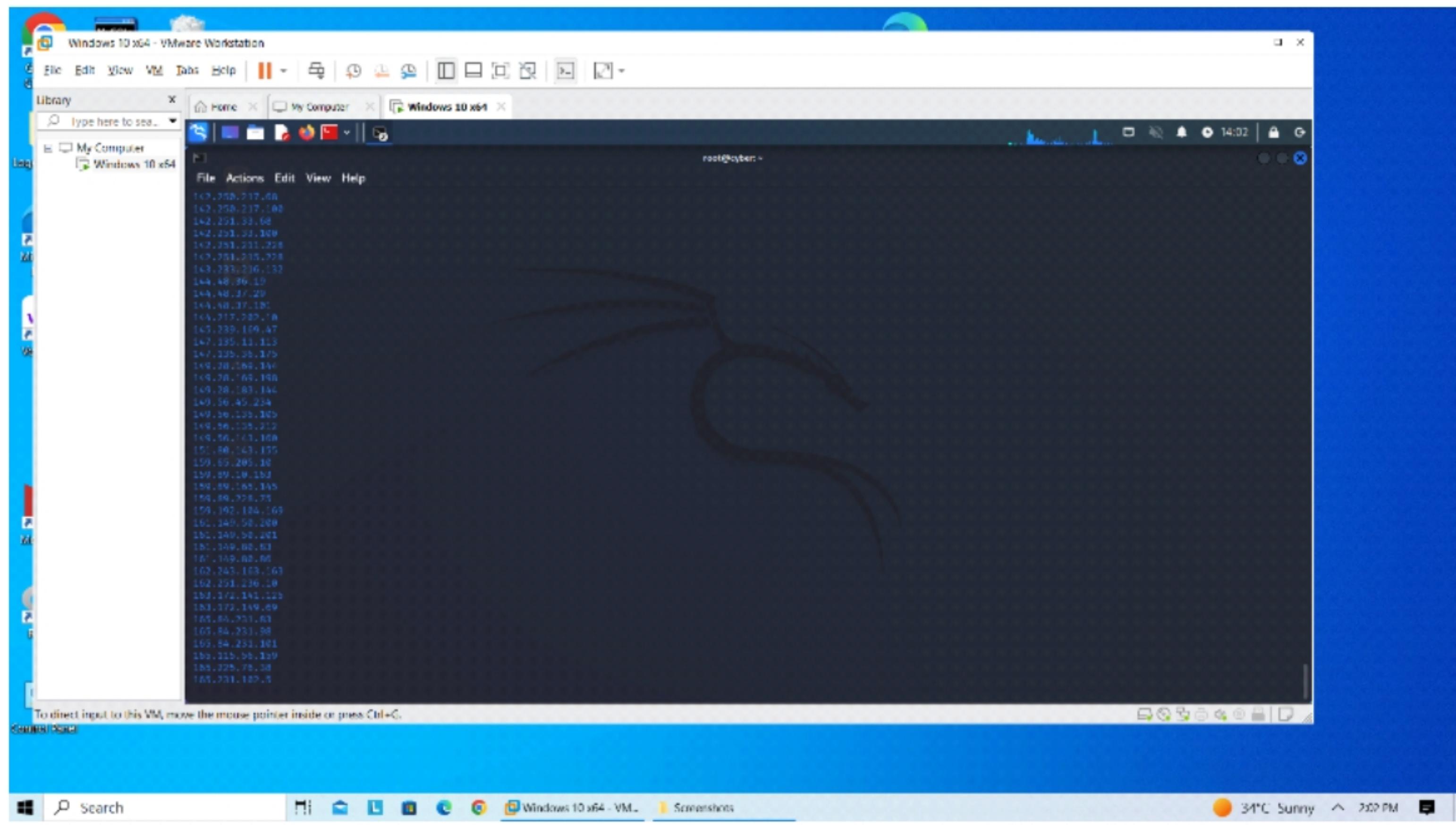
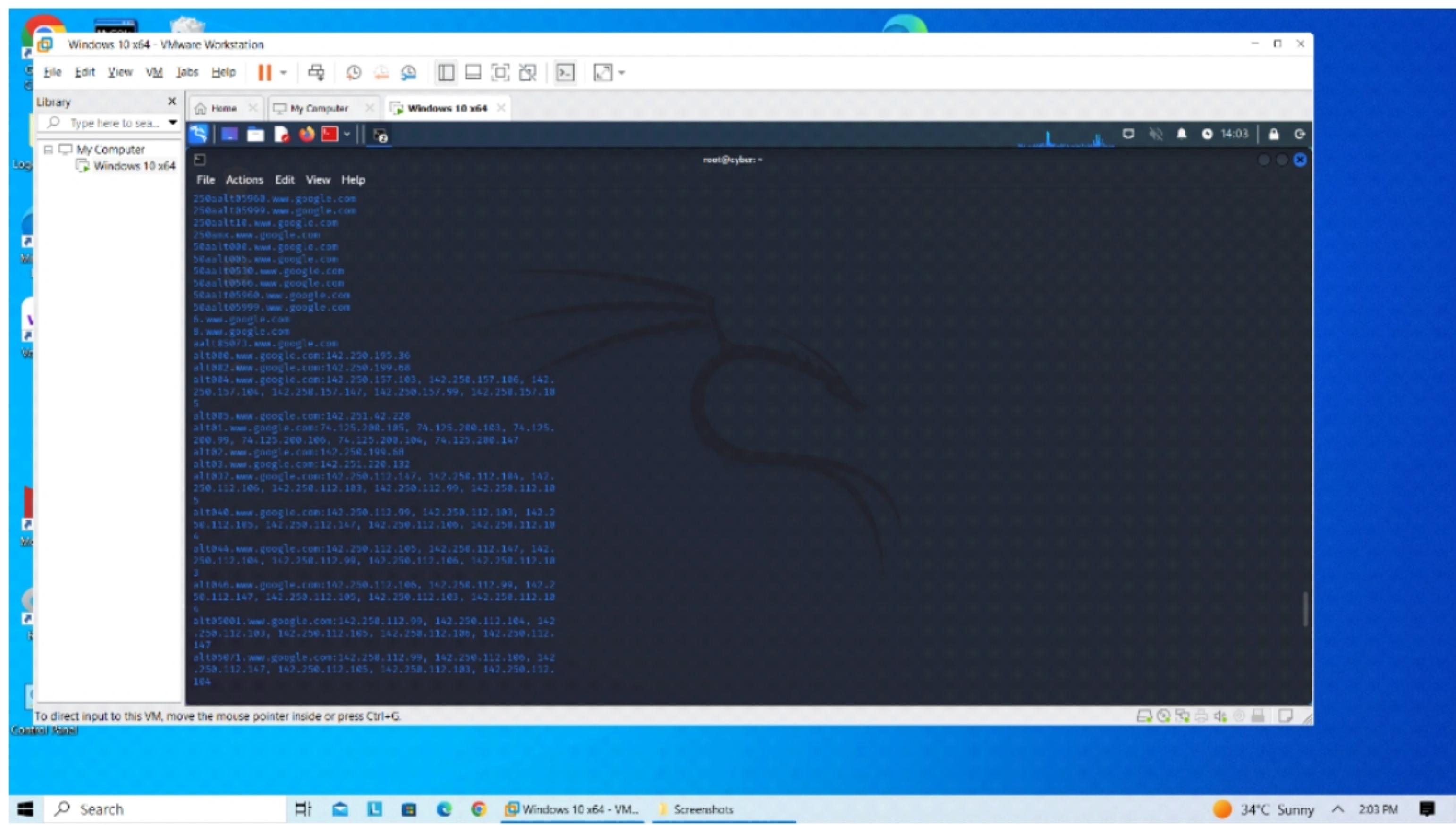
Nmap done: 1 IP address (1 host up) scanned in 34.42 seconds

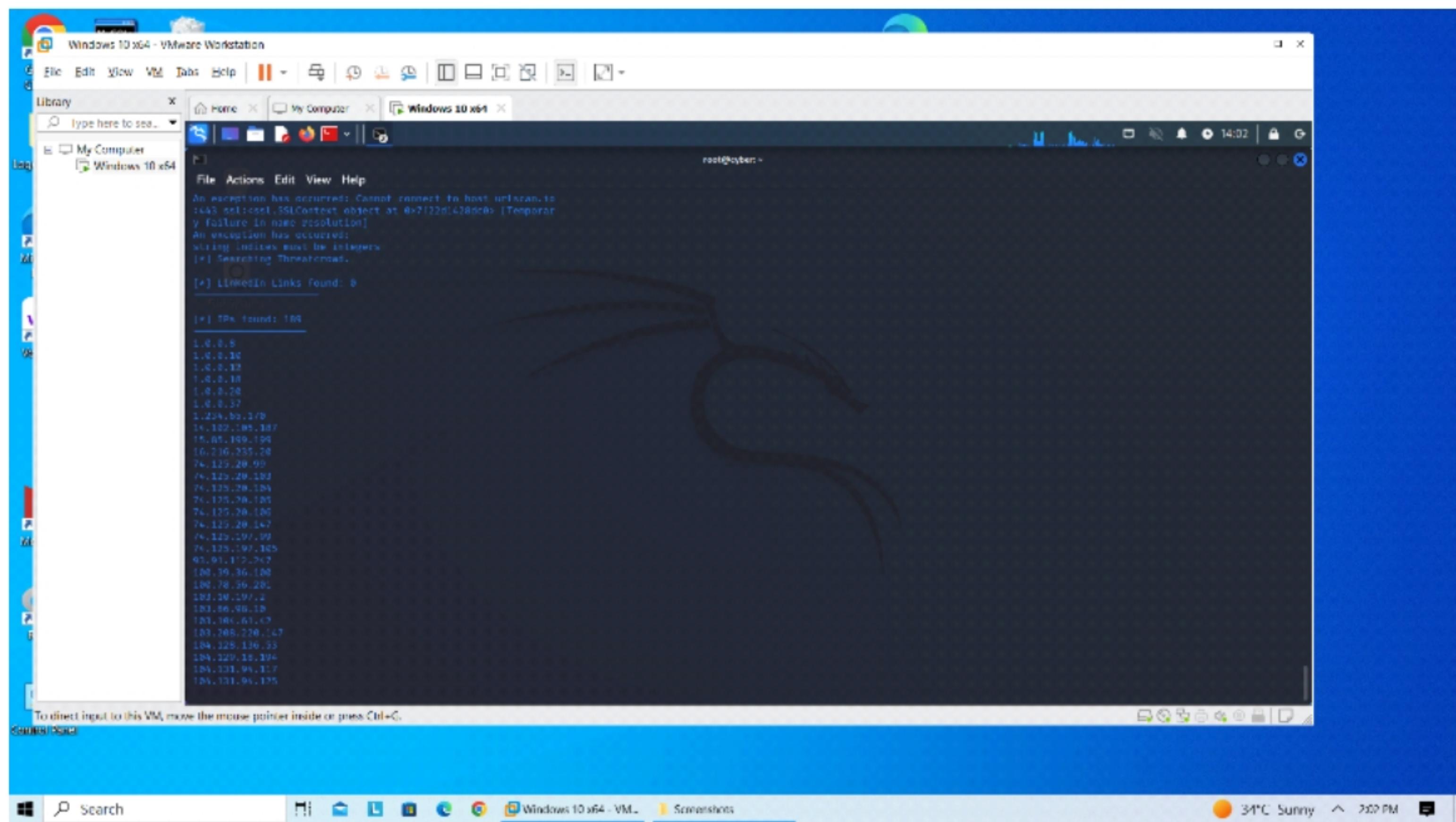
# nmap -O 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-19 13:50 IST
Nmap scan report for 192.168.1.1
Host is up (0.0024s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE      SERVICE
514/tcp   filtered  shell
Warning: OSscan results may be unreliable because we could n
ot find at least 1 open and 1 closed port
Device type: general-purpose
Running: Linux 2.4.X|3.X
OS CPE: cpe:/e:linux:linux_kernel:2.4..37 cpe:/e:linux:linux_
kernel:3.2 cpe:/e:linux:linux_kernel:4.4
OS details: ED WRT v4 sp2 (Linux 2.4..37), Linux 3.2, Linux
4.4

OS detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.49 seconds
```

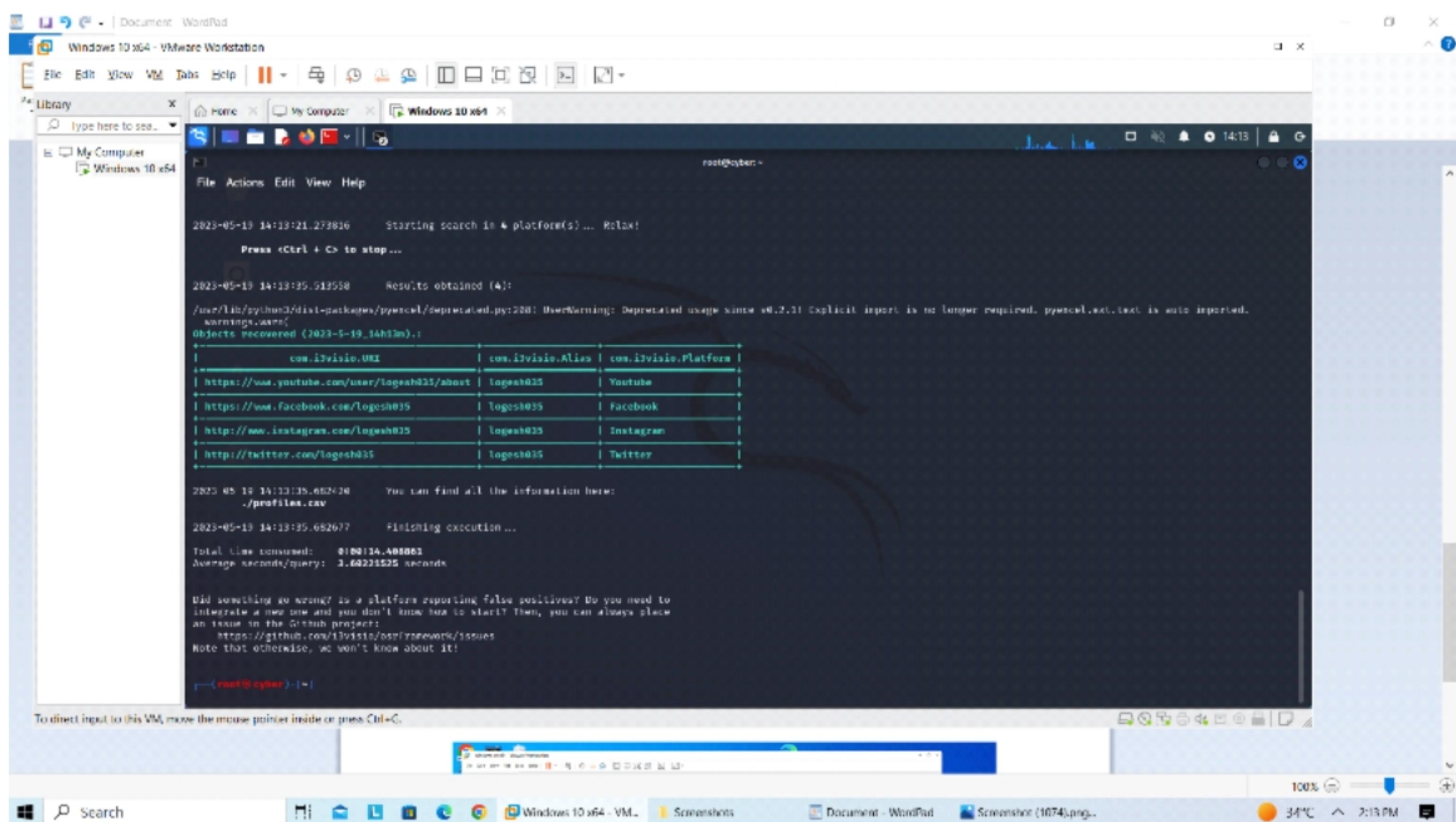
## 5. information gathering

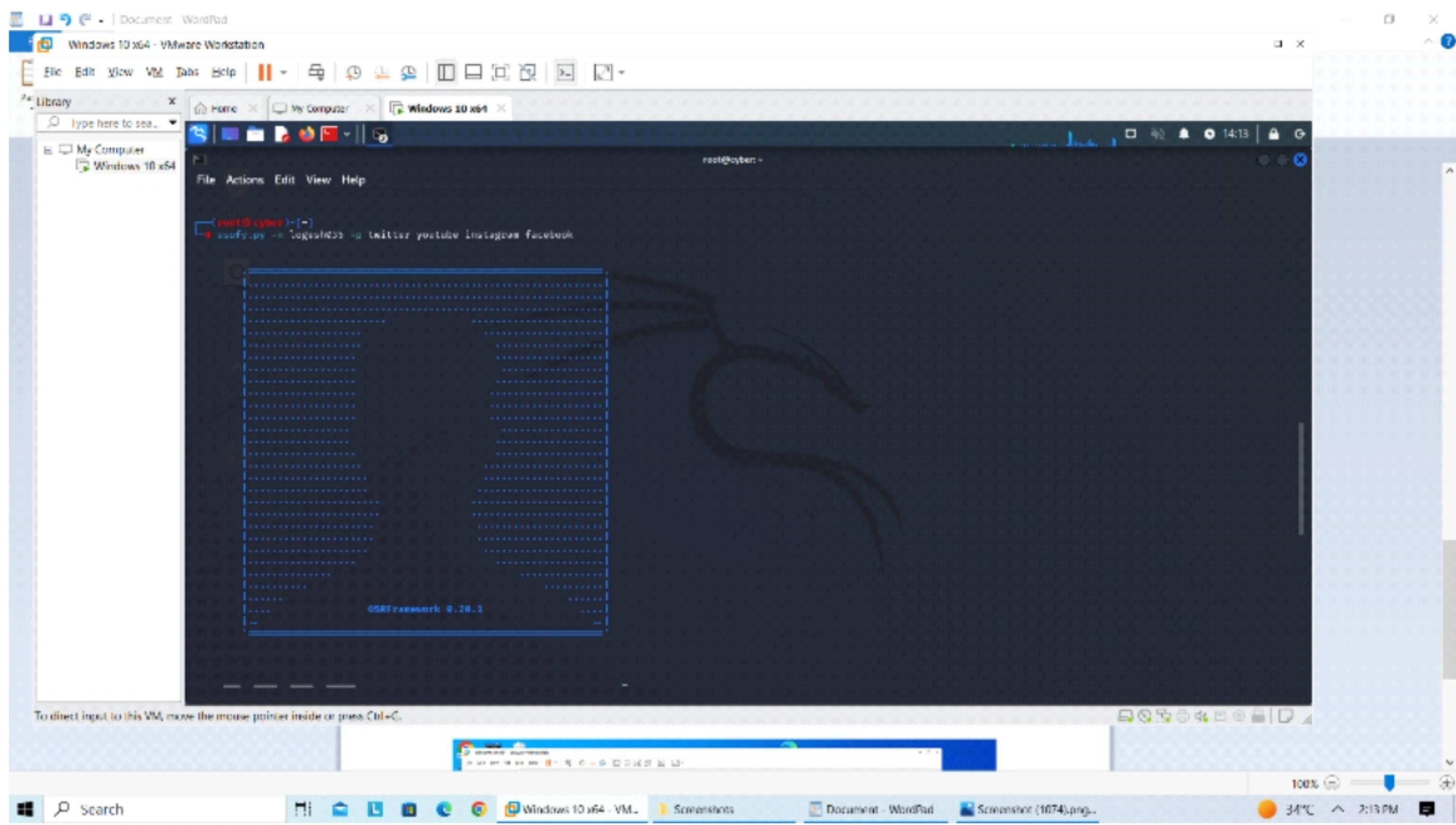
A screenshot of a Linux terminal window titled "Windows 10 x64 - VMware Workstation". The terminal is running as root on a Kali Linux virtual machine. The screen shows a list of IP addresses and hostnames, likely from a network scan or log file. The desktop background is visible behind the terminal window, showing a dark theme with a magnifying glass icon.



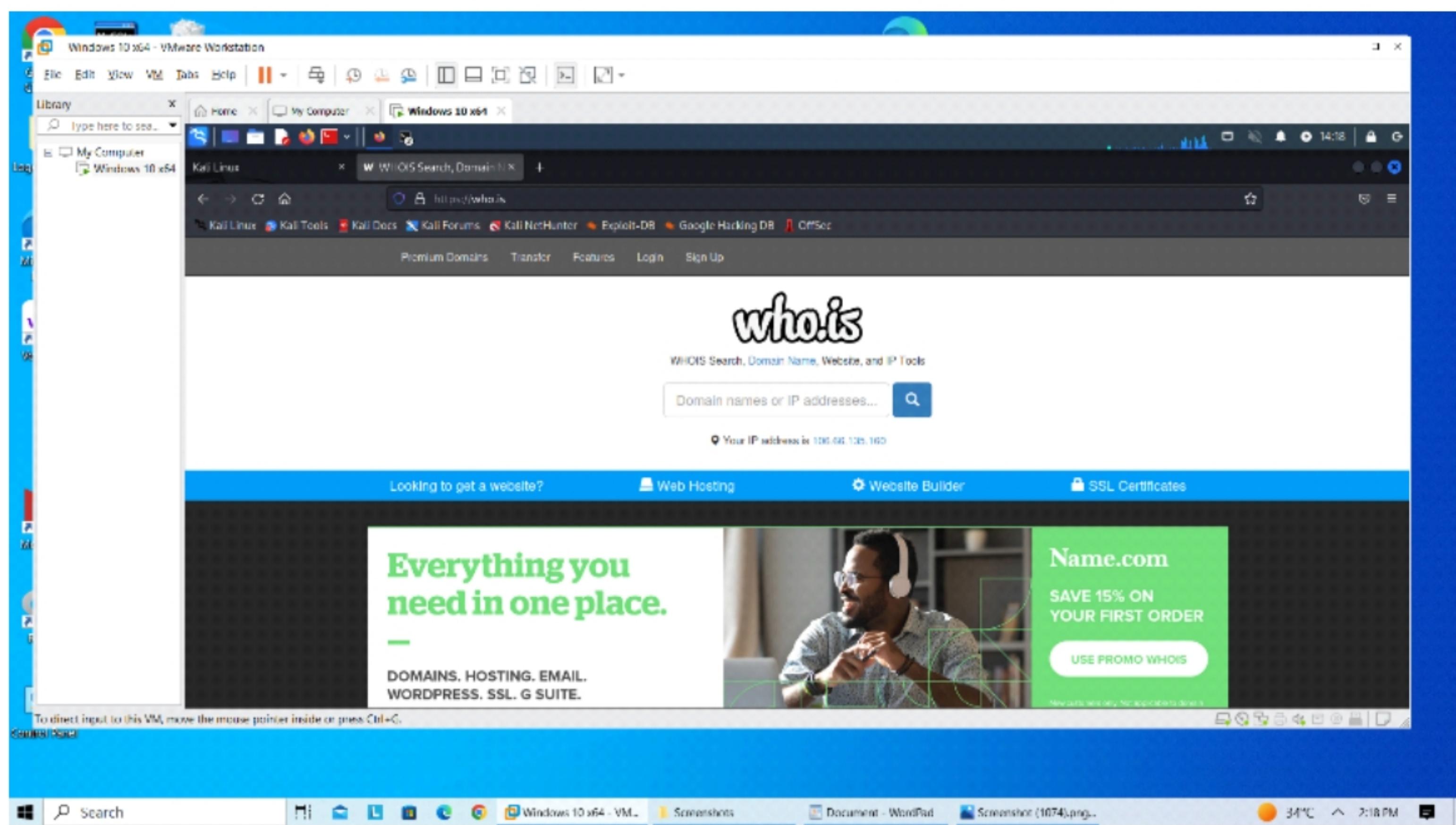


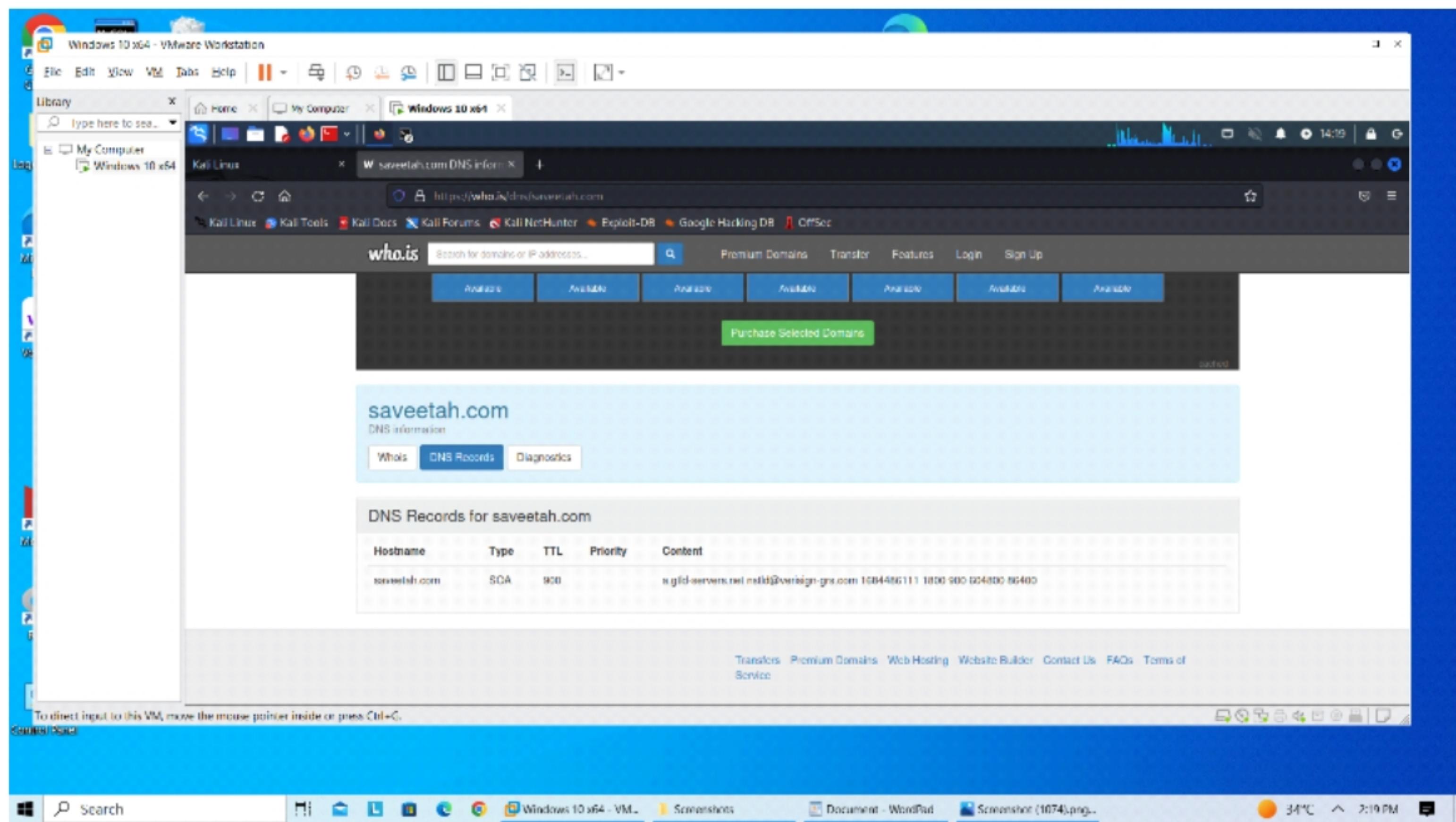
## 6. open source intelligence





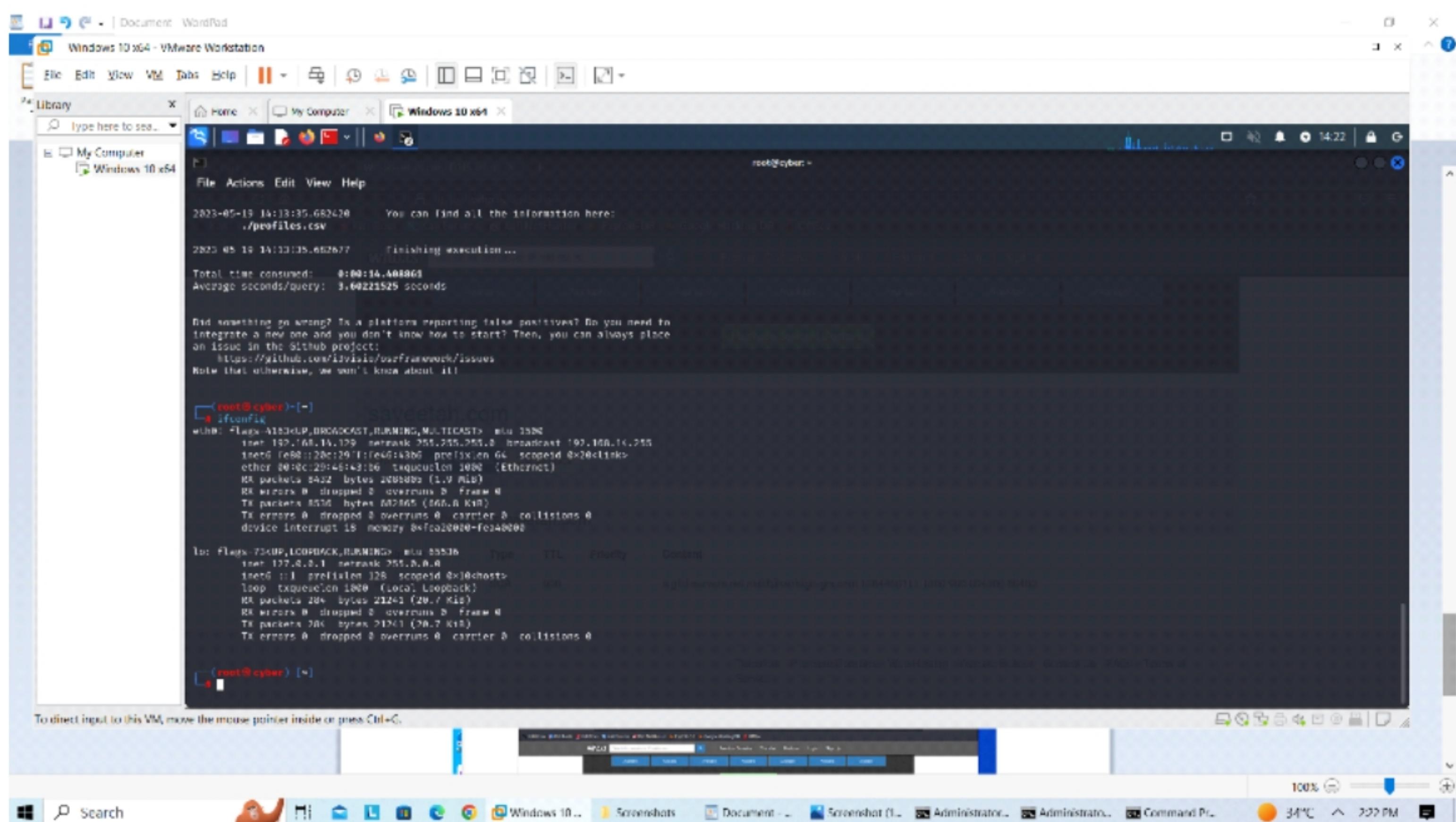
## 7 . use google whois for reconnaissance





## 8. tracert , ping , ipconfig if config

### ifconfig



### tracert

```
Administrator: Command Prompt for vhd - traceroute savetha.com
C:\Windows\system32>traceroute savetha.com
Tracing route to savetha.com [64.44.9.250] over a maximum of 30 hops:
 1  17 ms   3 ms   6 ms  2402:8100:2828:464d::fc
 2  117 ms   77 ms   76 ms  2402:8100:2::1::10a
 3  101 ms   82 ms   78 ms  2402:8100:2::1::10a
 4  250 ms   86 ms   77 ms  2402:8100:2::1::117
 5  *       *       * Request timed out.
 6  *       *       * Request timed out.
 7  *       *       * Request timed out.
 8  *       *       * Request timed out.
 9  *       *       * Request timed out.
10  *       *       * Request timed out.
11  *       *       * Request timed out.
12  *       *       * Request timed out.
13  *       *       * Request timed out.
```

ping

```
Administrator: Command Prompt for vhd
C:\Windows\system32>ping 17.18.43.1
Pinging 17.18.43.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 17.18.43.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Windows\system32>
```

netstat

Command Prompt for vct1

C:\Program Files (x86)\WinRAR\WinRAR-Master\bin\netstat -an

Active Connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:1411	1APTOP-TL5SRMRW:1412	FSTABITSHFD
TCP	127.0.0.1:1412	1APTOP-TL5SRMRW:1411	FSTABITSHFD
TCP	127.0.0.1:49684	1APTOP-TL5SRMRW:49685	FSTABITSHFD
TCP	127.0.0.1:49685	1APTOP-TL5SRMRW:49684	FSTABITSHFD
TCP	127.0.0.1:49686	1APTOP-TL5SRMRW:49687	FSTABITSHFD
TCP	127.0.0.1:49687	1APTOP-TL5SRMRW:49686	FSTABITSHFD
TCP	102.168.246.136:1833	ec2-54-208-226-89:https	FTN_MATT_1
TCP	102.168.246.136:1834	55:https	FSTABITSHFD
TCP	102.168.246.136:1846	201:https	TTMF_MATT
TCP	102.168.246.136:1854	184.208.16.9:https	FTN_MATT_1
TCP	102.168.246.136:1859	204:https	FTN_MATT_1
TCP	102.168.246.136:1868	www03s46-in-f8:https	FTN_MATT_1
TCP	102.168.246.136:1873	191:https	FTN_MATT_1
TCP	102.168.246.136:1148	www05s26-in-f1d:https	FTN_MATT_1
TCP	102.168.246.136:1161	www03s39-in-f6:https	FTN_MATT_1
TCP	102.168.246.136:1213	230:https	FSTABITSHFD
TCP	102.168.246.136:1226	52.196.90.28:https	TTMF_MATT
TCP	102.168.246.136:1233	40.65.111.94:https	TTMF_MATT
TCP	102.168.246.136:1239	52.196.147.113:https	TTMF_MATT
TCP	102.168.246.136:1241	52.196.147.113:https	TTMF_MATT
TCP	102.168.246.136:1333	www05s26-in-f2:https	FTN_MATT_1
TCP	102.168.246.136:1368	server-13-32-145-81:https	TTMF_MATT
TCP	102.168.246.136:1362	www05s26-in-f1d:https	FSTABITSHFD
TCP	[:]1:1494	1APTOP-TL5SRMRW:1495	FSTABITSHFD
TCP	[:]1:1495	1APTOP-TL5SRMRW:1494	FSTABITSHFD
TCP	128.81.99.2828:4544:ddde1:3d091:625d:1746j:1019	[64:ffff:14:6:7754]:https	FSTABITSHFD
TCP	128.81.99.2828:4544:ddde1:3d091:625d:1746j:1046	[2601:1988:2381:1+01c:1fe]:http	FSTABITSHFD
TCP	128.81.99.2828:4544:ddde1:3d091:625d:1746j:1188	[64:ffff:14:c4:5de]:https	FSTABITSHFD
TCP	128.81.99.2828:4544:ddde1:3d091:625d:1746j:1189	[2620:1e:11:200]:https	FSTABITSHFD
TCP	128.81.99.2828:4544:ddde1:3d091:625d:1746j:1195	[64:ffff:100:3:264c]:https	FSTABITSHFD
TCP	128.81.99.2828:4544:ddde1:3d091:625d:1746j:1196	[64:ffff:1736:52:0]:https	CLOSE_MATT
TCP	128.81.99.2828:4544:ddde1:3d091:625d:1746j:1198	[64:ffff:1736:52:0]:https	CLOSE_MATT
TCP	128.81.99.2828:4544:ddde1:3d091:625d:1746j:1201	[2605:1045::86:1d:2]:https	FSTABITSHFD
TCP	128.81.99.2828:4544:ddde1:3d091:625d:1746j:1204	[2605:1045::86:1d:2]:https	FSTABITSHFD
TCP	128.81.99.2828:4544:ddde1:3d091:625d:1746j:1210	[2605:2808:147:120+30c:1fe:6:265a]:https	FSTABITSHFD
TCP	128.81.99.2828:4544:ddde1:3d091:625d:1746j:1211	[2605:2808:147:120+30c:1fe:6:265a]:https	FSTABITSHFD
TCP	128.81.99.2828:4544:ddde1:3d091:625d:1746j:1212	[2605:2808:247:6711:6f8:1d37:eed5:e137]:https	FSTABITSHFD
TCP	128.81.99.2828:4544:ddde1:3d091:625d:1746j:1242	[64:ffff:dd5b:55h]:https	FSTABITSHFD
TCP	128.81.99.2828:4544:ddde1:3d091:625d:1746j:1243	[64:ffff:dd5b:3fe]:https	FSTABITSHFD
TCP	128.81.99.2828:4544:ddde1:3d091:625d:1746j:1244	[64:ffff:dd5b:3fe]:https	FSTABITSHFD
TCP	128.81.99.2828:4544:ddde1:3d091:625d:1746j:1245	[64:ffff:dd5b:6fe]:https	FSTABITSHFD
TCP	128.81.99.2828:4544:ddde1:3d091:625d:1746j:1246	[2601:1988:2381:dd9c:1fe]:http	FSTABITSHFD

C:\Program Files (x86)\WinRAR\WinRAR-Master\bin\netns

Search Home Mail File Explorer Edge Google Windows 10 Screenshots Document - Word Screenshot (107...) Administrator Command Prom... 34% 223 PM

## 9. vulnerability cgi scanning

The screenshot shows a terminal window titled "Windows 10 x64 - VMware Workstation" running on a Windows host. The terminal is displaying the output of a Nikto web vulnerability scanner against the target website `saveetha.com`. The results are as follows:

```
(root㉿cyber)-[~]# nikto -h saveetha.com -Tuning
- Nikto v2.1.6

+ Target IP:          198.185.159.146
+ Target Port:        80
+ Message:           Multiple IP addresses found: 198.185.159.144, 198.185.159.145
+ Start Time:        2023-05-19 14:28:27 (GMT+5.5)

+ Server: Squarespace
+ Cookie crumb created without the httpsonly flag
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Unknown header 'x-content-type' found, with contents: vNM7frsk/PerFMg9n
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the HTML type
+ Root page / redirects to: https://www.saveetha.com/
^C

(root㉿cyber)-[~]# nikto -h saveetha.com -Gidirs all
- Nikto v2.1.6

+ Target IP:          198.185.159.146
+ Target Port:        80
+ Message:           Multiple IP addresses found: 198.185.159.144, 198.185.159.145
+ Start Time:        2023-05-19 14:28:15 (GMT+5.5)

+ Server: Squarespace
+ Cookie crumb created without the httpsonly flag
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Unknown header 'x-content-type' found, with contents: sp5Yzckw/m3w0X51Q
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the HTML type
+ Root page / redirects to: https://www.saveetha.com/
^[[2;1~C

[root@cyber] ~]
```

To direct input to this VM, move the mouse pointer inside or press **Ctrl+C**.

### 3.. wireshark

